



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,864	08/20/2003	Masayuki Nakae	8046-1041	5195
466 7590 02/05/2008 YOUNG & THOMPSON 745 SOUTH 23RD STREET 2ND FLOOR ARLINGTON, VA 22202			EXAMINER BROWN, CHRISTOPHER J	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 02/05/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/643,864

Applicant(s)

NAKAE ET AL.

Examiner

Christopher J. Brown

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 29 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-13 and 113-143 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13, 113-143 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |                                                                                                                                         |                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                                                                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                                    | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>8/8/07, 11/19/03</u> | 6) <input type="checkbox"/> Other: _____                                                |

## DETAILED ACTION

### *Response to Arguments*

Applicant's arguments filed 10/29/07 have been fully considered but they are not persuasive.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Lachmen may not teach forwarding packets from a router, but it is well known in the art that routers may forward packets to other devices.

It is well known in the art to introduce malicious code over a network. Sheymov teaches receiving malicious code and studying the effects on a decoy system. The applicant asserts that a "network service process" is not executed in response. The Examiner asserts that "network service process" must be interpreted with the broadest reasonable interpretation. Under said interpretation, scanning the packets or code and cleaning or eliminating them are network service processes. The examiner invites the applicant to specify which network service processes the applicant intends in the claim language.

***Information Disclosure Statement***

Information Disclosure Statements filed 11/19/03, and 8/8/07 have been considered. No English translation, or other description for the IDS filed on 10/7/05 can be found on Public Pair or at the PTO.

***Claim Rejections - 35 USC § 101***

The claimed invention is directed to non-statutory subject matter.

Claims 1, 113, 117, 121, 126, 133, 138, 143 and dependent claims are directed towards non-statutory subject matter. The independent claims interpreted with the broadest reasonable interpretation result in the independent claims being pure software. The applicant must claim that the functions are performed in hardware, in line with the instant specification, including processors, and or computer readable medium.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 126 and 143 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lachman III US 2002/0166063 in view of Sheymov US 7,010,698.

As per claims 1, and 59 Lachman teaches an attack defending system provided at an interface between an internal network (host network) and an external network (internet), comprising a decoy device and a firewall device (Uplink Router), wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device (Host router) and the internal network (Host Server, ANT Surveillance System),

the firewall device comprises: a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet (filter with source address of packet) [0125] and a filtering condition corresponding to the input IP packet; a destination selector for selecting one of the internal network (Host Server) and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device (Updates ACL based on attack detection). Lachman III fails to teach a decoy device that comprises an attack detector.

Sheymov teaches wherein the decoy device comprises: an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, (Dynamic Decoy Device with Sensor Module to detect attacks) (Col 8 lines 4-8).

It would have been obvious to one of ordinary skill in the art to use the attack detection decoy of Sheymov with the system of Lachman III because it removes the need for additional attack detection devices thus lowering cost.

As per claim 2, 127 Lachman III teaches attack defending system according to claim 1, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof (It is well known TCP/IP packets contain source and destination IP addresses in the header), wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition (based on an access control list of source and IP addresses) [0125], [0133], [0135].

As per claim 5, 128 Lachman III teaches the attack defending system according to claim 1, wherein the firewall device further comprises: a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device (Offensive Countermeasure Server updates router) [0076], [0116].

As per claim 6, 129 Lachman III teaches the attack defending system according to claim 1, wherein the filtering condition manager stores the filtering condition with a limited validity period, (specified time) [0125] which corresponds to the header information of the input IP packet (access control list) forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

*Allowable Subject Matter*

Claims 3, 4, 7-13, and 130-132 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 113, 117, 121, 133, and 138 are allowable over the prior art of record if the USC 101 rejection is overcome.

*Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

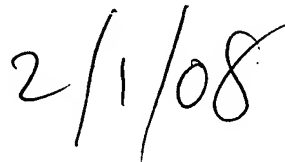
Application/Control Number:  
10/643,864  
Art Unit: 2134

Page 7

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown

2/1/08

A handwritten signature in black ink, appearing to read "Chris Brown", written in a cursive style.A handwritten date "2/1/08" in black ink, written in a cursive style.